Information
and Privacy
Commissioner/
Ontario

Submission to the Standing Committee on General Government:

Bill 159: Personal Health Information Privacy Act, 2000

Ann Cavoukian, Ph.D.
Commissioner
February 2001

101-04034/

Information and Privacy
Commissioner/Ontario

80 Bloor Street West
Suite 1700
Toronto, Ontario
M5S 2V1

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Web site: http://www.ipc.on.ca

This publication is also available on the IPC Web site.

Table of Contents

Introduction 1

Part I: Purposes, Definitions and Interpretation 2
- Definition of Personal Health Information 2

Part II: Application of the Act 3
- Anonymous Health Information 3
- Information Relating to Labour Relations and Employment Matters 3

Part III: General Limitations 4
- Electronic Use of Information 4
- Computer Matching 5
- Limitations on Employees 6

Part IV: Practices to Protect Personal Health Information 7
- Written Policies 7
- Information for the Public 7

Part V: Consent 8
- Elements of Consent 8

Part VI: Collection, Use and Disclosure of Personal Health Information 9
- Limits on Collection 9
- Notice of Purpose 9
- Information about Uses and Disclosures 10
- Limits on Marketing 10
- Permitted Uses 11
- Disclosures Related to the Individual 11
- Disclosures about a Deceased Individual 12
- Disclosures for Health or Other Programs 13
- Disclosure by the Minister 13
- Disclosures Directed by the Minister 14
- Disclosures for Research 15
- Use and Disclosure Outside Ontario 17

Part VIII: Access to Records of Personal Health Information 18
- Access to Records 18
- Amendment of Record 19

Part X: Powers and Duties of the Commissioner 21
- Powers 21
- Delegation 21

Part XI: Administration and Enforcement 22
Complaints 23
Inquiry 24

Part XII: Miscellaneous 26
Regulations 26

Additional Recommendations 27
Privacy Impact Assessment 27

Conclusion 28

Introduction

The Office of the Information and Privacy Commissioner of Ontario (IPC) has a mandate under the Freedom of Information and Protection of Privacy Act to review and comment on the privacy implications of proposed legislative schemes. Bill 159, the Personal Health Information Privacy Act, 2000 (the Act) will have a significant impact on the privacy of every individual in the province of Ontario.

We are pleased that the Government has taken the important step of introducing a comprehensive legal framework to protect personal health information. Our office has advocated the need for such legislation for many years. Members of the public, health care providers and other stakeholder groups have anticipated introduction of legislation of this nature since the Report of the Royal Commission on Confidentiality of Health Information in Ontario (the Krever Commission Report) in 1980.

We also are pleased that this office has been identified as the oversight body for this legislation. Having one oversight body for all privacy legislation in Ontario provides the public with a single point of contact for both access and privacy matters. This will facilitate implementation of the legislation and minimize confusion on the part of the public.

While we generally support the introduction of this legislation, we believe it must be strengthened in a number of key areas. Our main recommendations focus on three areas of concern:

- putting limits on disclosures of personal health information without consent, particularly for purposes related to the management of the health system;
- reducing the broad regulation-making powers provided by the legislation that could potentially diminish the privacy protection provided by the legislation; and
- providing the Commissioner with sufficient powers to effectively and efficiently oversee and enforce the legislation.

The comments and recommendations in this submission support three primary goals – to enhance the privacy protections provided by the legislation; to promote harmonization of this legislation with federal privacy legislation and with other provincial health information privacy legislation; and to facilitate implementation, administration and enforcement of the legislation. Our comments are organized in accordance with the corresponding parts of the legislation.

Part I: Purposes, Definitions and Interpretation

In general, we support the purposes of the legislation identified in section 1. These purposes recognize the unique character of personal health information – as one of the most sensitive types of personal information that is frequently used and disclosed for a broad range of purposes that go beyond the provision of health care to the individual.

Definition of Personal Health Information

While we generally support the definitions and interpretation as set out in subsection 2(1), we have some concerns about the wording of the definition of "personal health information." The definition seems to suggest there are two distinct types of information that fall within the definition – information that relates to an identifiable individual as set out in paragraph (a), and information that relates to the individual's health care as set out in paragraph (b). It is our understanding that the information must fulfill the criteria in both (a) and (b) before it would be considered to fall within the definition. Specifically, information must relate to an identifiable person and it must be about his or her health or health care, rather than just one or the other. This should be clarified.

A related issue is the inclusion of provider information in paragraph (b)(viii) of the definition. It is our view that information about the employment and business responsibilities, activities and transactions of individual health service providers should not be included in the definition of personal health information. This type of information may be used to objectively assess the quality of provider services and should be considered professional in nature rather than personal health information. Since it is not clear under the definition of personal health information that the information must be personally identifiable as required under paragraph (a), paragraph (b)(viii) could be interpreted as applying to provider information that is linked to any health information, whether it is personally identifiable or not. To ensure that paragraph (b)(viii) is not construed to protect provider information that is linked to any health information, the definition of personal health information should be worded in a manner such that it is clear that information must meet the criteria in both (a) and (b) rather than (a) or (b).

In addition, it is our view that the definition of personal health information should include a record of disclosures of personal health information that each custodian should be required to keep under the legislation. Custodians are required to document anticipated uses and disclosures and make a note of unanticipated uses and disclosures of personal health information, under the circumstances prescribed in the regulations. However, in our view this is not sufficient. To ensure openness and transparency, custodians should be required to keep a record of both routine and non-routine uses and disclosures of personal health information. This record should be included in the record of personal health information to which the individual has access. This would be consistent with Alberta's Health Information Act.

Part II: Application of the Act

Anonymous Health Information

As specified in paragraph (c) of section 7, we agree that the privacy rules set out in the legislation should generally not apply to truly anonymized information. However, the legislation should recognize that, in some cases, due to an individual's unique characteristics, it may be possible to identify the individual from anonymized health information. In other cases, it also may be possible to de-anonymize seemingly anonymous health information by linking it to publicly available information about individuals. In light of these potential threats to privacy, it is our view that the legislation should include some safeguards for anonymous health information.

Specifically, the legislation should require custodians to ensure that anonymous health information is:

- only used and disclosed for health-related purposes;
- not combined or linked to any other information that would permit the anonymous individual to be re-identified; and
- not published in a manner that could be used to identify an individual (e.g., small cells of data).

Information Relating to Labour Relations and Employment Matters

Paragraph 7(d) puts limits on individuals' ability to access their own personal health information when it relates to certain labour relations or employment-related matters. We recommend omitting this limitation from the legislation. In our view, this paragraph places unjustified limits on individuals' right to access to their own personal health information and would be inconsistent with the federal private sector privacy legislation, the Personal Information Protection and Electronic Documents Act.

Part III: General Limitations

Section 12 contains the general limitations on the collection, use and disclosure of personal health information. However, under subsection 12(8), personal health information that is required to be disclosed under this Act, is exempted from the general limiting principles. One of the required disclosures under the Act is where the Minister of Health and Long-Term Care directs a custodian to disclose personal health information under section 31, for purposes related to management of the health system. In such circumstances, the general limitations, such as the requirement to limit the amount of personal information that is disclosed, will not apply. We recommend these general limitations on the collection, use and disclosure of personal health information should apply to all disclosures permitted without the consent of the individual, including disclosures directed by the Minister.

Electronic Use of Information

Section 13 relates to electronic use of information. It states that a health information custodian shall comply with the requirements prescribed by the regulations with respect to the electronic transfer of personal health information. Since the electronic sharing of personal health information raises major privacy issues, we recommend that safeguards for the electronic use of personal health information be set out in the legislation rather than in the regulations. This would permit public debate about the important privacy issues that are raised.

In an electronic world, the individual's ability to control what information is disclosed is essential for privacy protection. New information management and telecommunications technology allow for the creation of an electronic patient record containing a cradle-to-grave medical history that can be readily shared among a variety of health care providers, and beyond, with the push of a button. Since the electronic patient record will be accumulated over a much longer period of time than most paper-based medical records, the likelihood that it will contain outdated and perhaps irrelevant information is increased. Also, in comparison to most paper-based medical records, the cradle-to-grave electronic patient record is more likely to contain sensitive information that the person does not want widely shared. For example, it might contain information about abortions, sexually transmitted diseases, sexual orientation, substance abuse, psychological problems, etc. While this type of information might be critical in some health care situations, in other circumstances, it may not be relevant.

If individuals have no control over the personal health information contained in their electronic patient record or how that information is disclosed, they may engage in activities to prevent information from being added to their record. For example, individuals could withhold certain sensitive information or provide inaccurate information out of fear that the information will make its way onto their electronic patient record and could be made indiscriminately available to all of their

health care provider sor, perhaps, other secondary users of personal health information. In addition, individuals who have concerns about the use and disclosure of their health information may avoid seeking treatment altogether. If the electronic patient record contains inaccurate or incomplete information, its usefulness for providing health care to the individual and for secondary purposes (e.g., planning and research) would be significantly diminished.

Under Alberta's Health Information Act, a custodian must obtain the individual's consent before disclosing personal health information by electronic means, for purposes other than billing. Under Saskatchewan's Health Information Protection Act, individuals have the right to require a custodian not to store a record or any part of a record on the networked electronic health record maintained by the government or any other prescribed network. In addition, where information is stored on the electronic health record, an individual may require a custodian to prevent access by other custodians to all or part of that information from the network. These are important privacy safeguards for health information networks. It is our view that unless such safeguards for the electronic use of personal health information are incorporated into Ontario's legislation, the adoption of new information management and telecommunications technology in the health sector will be seriously impeded by concerns about privacy.

Computer Matching

While we are pleased that requirements for computer matching have been set out in the legislation rather than in regulations, we have a number of concerns about the substance of the requirements. Computer matching is an error-prone procedure that is generally used to generate new information about the individual through the linking of two or more databases. This new information is used to make administrative decisions that may directly affect individuals.

The requirements for computer matching set out in the legislation were drawn from the computer matching directive of Management Board Secretariat. However, there are some significant discrepancies between the requirements under the directive and those under the legislation. First, subsection 14(3) of the legislation lists a number of exceptions to the application of the computer matching requirements. However, under the computer matching directive, these are not exceptions to the rules but examples of situations in which the directive generally does not apply. These examples were included in the directive to illustrate some of the situations where computer matching may be used, but not for a purpose that directly affects the individual. It is our understanding that the computer matching procedure would be excluded from the requirements of the directive only if the computer match was being undertaken solely for one or more the purposes mentioned in the examples. Accordingly, if the computer matching procedure fits the criteria set out under subsection 14(2) of the legislation, the computer matching requirements should apply. There should be no exceptions to this.

In addition, all of the requirements of the computer matching directive of Management Board Secretariat should be included in the legislation. For example, under the directive, government organizations are required to independently verify that the information produced by the computer match is correct. Procedures for verifying information must be set out in the computer matching assessment provided to the Information and Privacy Commissioner. Since computer matching is an imprecise procedure, before any action is taken against the individual based on the computer matching procedure, independent verification of information is essential. However, this important privacy safeguard in the directive has been left out of the computer matching requirements in the legislation.

In our view, safeguards for the use and disclosure of personal health information for computer matching purposes should apply to all personal health information, not just that which is in the custody of government organizations. This would be consistent with the requirements of Alberta's Health Information Act which contains provisions requiring all health information custodians to prepare a privacy impact assessment and submit the assessment to the Information and Privacy Commissioner before performing data matching.

Finally, for the purposes of transparency and accountability, we recommend that all computer matching assessments and any comments offered by the Information and Privacy Commissioner be made available to the public.

Limitations on Employees

Section 16 of the legislation sets out limitations on the collection, use, disclosure, retention and disposal of personal health information by persons employed by or in the service of the custodian. In order to emphasize that the range of individuals who have access to personal health information should be as restricted as possible, subsection 16(2) should limit the collection, use and disclosure of personal health information to those who need the information for the performance of their duties with or on behalf of the custodian. Specifically, paragraph (b) should state that the collection, use, disclosure or disposal of the information must be necessary in the course of the person's duties.

Part IV: Practices to Protect Personal Health Information

Written Policies

Subsection 19(1) requires a health information custodian to have a written policy concerning the retention and disposal of records. This is not sufficient. While a written policy on the retention and disposal of records is an essential first step, the custodian also should be required to establish or adopt written policies and procedures that will facilitate the implementation of all aspects of the legislation and the regulations, including the collection, use and disclosure of personal health information. For example, Alberta's Health Information Act contains a provision requiring each custodian to establish or adopt policies and procedures that will facilitate the implementation of the legislation. Saskatchewan's Health Information Protection Act requires a trustee to establish policies and procedures to promote knowledge and awareness of the rights extended to individuals by the legislation, including the right to request access and correction of personal health information.

Information for the Public

In general, we are pleased the legislation will require each custodian to designate a contact person. Specifically, subsection 20(1) requires a custodian to designate an individual or individuals to facilitate the custodian's compliance with the legislation; to ensure that employees are informed of their duties under the legislation; to respond to inquiries from the public about the custodian's information practices; and to receive complaints from the public about alleged contraventions of the legislation. We suggest this person also should receive requests to access and correct personal health information. This would enhance customer service by providing a single contact person for all access and privacy matters.

Subsection 20(2) sets out what must be contained in a statement that the custodian must make available to the public upon request. This statement must describe the custodian's information practices; how to contact the person described above; how to obtain access to records; and how to make a complaint to the Commissioner. We recommend that this statement also describe how to complain to the custodian about an alleged contravention of the Act, the regulations or the custodian's information practices. This would provide custodians with an opportunity to resolve any privacy issues before a formal complaint is made to the Commissioner. In addition, we recommend that the legislation contain a requirement for custodians to inform individuals, at the time when personal health information is collected, that they may request a copy of this statement. (See recommendations relating to the notice requirements under section 22(5).)

Part V: Consent

Elements of Consent

We are pleased that the legislation includes guidance on what constitutes informed consent. However, the requirements for informed consent for the collection, use and disclosure of personal health information should be strengthened. Subsection 21(1) contains the requirements for the collection, use or disclosure of personal health information. Paragraph (b) states that the consent must relate to the information. To ensure that consent to collect, use or disclose personal health information relates to the specific information, and not all of the individual's health information, we recommend that paragraph (a) should refer to the specific information.

Subsection 21(3) describes some information that may be provided when obtaining consent. This subsection could be strengthened by requiring this information to be part of the consent. In addition to the information specified in subsection 21(2), the consent should include a statement that the individual may specify a time after which the consent will cease to be effective (as provided for under subsection 21(5)), and a statement that the individual may revoke it at any time (as provided for under subsection 21(7)). Such requirements would make Ontario's legislation more consistent with health information legislation from other jurisdictions, such as the province of Alberta.

Subsection 21(4) states that a consent shall not be deemed to have been given involuntarily solely because it was given so that the individual would be eligible to receive a statutory benefit. Although we understand the purpose for this subsection, it should be noted that the provision contradicts some fundamental principles of informed consent. This type of provision would be unnecessary if appropriate criteria for what constitutes informed consent were included in the legislation. Specifically, the legislation should specify that the individual providing the consent should be made aware of the benefits and risks to the individual of consenting or refusing to consent. One of the potential risks would be ineligibility to receive a statutory benefit. If there were a requirement to inform the individual about the benefits and risks, this subsection could be deleted.

We question the necessity of subsection 21(8) which permits a custodian who receives a consent for the collection, use or disclosure of personal health information to assume it is valid, unless it is not reasonable to assume so. This provision seems to remove any onus on the custodian to take reasonable steps to ensure that a consent fulfills the requirements of the legislation. Accordingly, we recommend that this provision be removed from the legislation.

Part VI: Collection, Use and Disclosure of Personal Health Information

Limits on Collection

Subsection 22(1) states that a custodian cannot collect personal health information unless it is authorized by or under an Act or necessary for a lawful purpose related to a function or activity of the custodian. In our view, the collection of personal health information should be allowed only where it is required by law or necessary for a lawful purpose related to a function or activity of the custodian. The custodian should not be allowed to collect personal health information simply because it is permitted by or under an Act, unless it is also necessary for the functions or activities of the custodian. This would be consistent with the restrictions on collection imposed under the Personal Health Information Act of Manitoba.

Notice of Purpose

Under subsection 22(5), when personal health information is collected, the custodian is required to inform the individual of the purpose or purposes for which the information is being collected, unless it is reasonable to infer them in the circumstances. This is not sufficient to ensure transparency of the information practices of custodians.

In light of the wide array of uses and disclosures of personal health information that are permitted without the consent of the individual, the legislation must ensure that individuals are informed about all anticipated uses and disclosures of their personal health information, at the time of collection. Section 25 requires the custodian to provide the individual with information about anticipated uses and disclosures and to make a note of unanticipated uses and disclosures of personal health information, in the circumstances set out in the regulations. However, there is no requirement for the custodian to inform individuals that information about anticipated uses and disclosures is available, and that unanticipated uses and disclosures will be noted in their record of personal health information.

In addition, section 20 requires a custodian to designate a contact person and to make available to the public a statement to promote openness and transparency in the custodian's information practices. However, there is no requirement for the custodian to provide members of the public with information about the contact person and the availability of this statement. Individuals should be made aware of this information at the time when personal information is collected.

Information about Uses and Disclosures

Subsection 25(1) requires a custodian who uses or discloses personal health information to provide the individual with information about the uses and disclosures the custodian expects to make, but only in the circumstances prescribed by the regulations. Section 25(2) requires a custodian to make a note of unanticipated uses and disclosures of personal health information, but only in the circumstances prescribed by the regulations. This implies that the custodian would only have to provide this information or make a note of this information, in some circumstances, as prescribed in the regulations.

This approach is not as clear or straightforward as the approach taken in most other privacy legislation. It is customary for privacy legislation to set out the basic privacy rules and to specify any exceptions to these rules directly in the legislation. In contrast, under section 25, the circumstances under which the basic privacy rules will apply are to be prescribed in the regulations. This suggests that, as a default, custodians will generally not be required to provide information about anticipated uses and disclosures, or to make a note of unanticipated uses and disclosures of personal health information. To ensure transparency and openness, we recommend that, as the default, custodians should be required to provide information about all anticipated uses and disclosures, at the time of collection, and to make note of all unanticipated uses and disclosures. In addition, to ensure adequate public scrutiny, any exceptions to these general rules should be set out in the legislation rather than in the regulations.

Limits on Marketing

We are pleased subsection 26(1) of the legislation contains a general prohibition against the use of personal health information for marketing purposes without the consent of the individual. We also support the limitations on the use and disclosure of personal health information for fundraising. Specifically, the legislation states that the custodian may only use or disclose an individual's name and address for fundraising purposes. Diagnostic or treatment information should not be used or disclosed for these purposes.

We are concerned that the legislation is not specific enough about the manner in which the custodian must provide individuals with an opportunity to request that the custodian not use their name and address for the purpose of fundraising activities. First, the custodian should be required to provide individuals with a simple means of opting out. Second, if individuals request that their names and addresses not be used for this purpose, the custodian should be required to delete those names and addresses from any mailing lists and to keep a written record of who has opted out to ensure that those individuals are never contacted for this purpose in the future.

Permitted Uses

The permitted uses of personal health information are set out under section 27. This section provides for the use of information without the consent of the individual. In order to enhance privacy, the permitted uses without consent should be as narrow as possible. Paragraph (k) permits the use of the information if it is permitted or required under another Act. Since the legislation already provides for a broad range of uses of personal health information without the consent of the individual, any additional uses authorized by another Act should be limited to those which are required rather than permitted by another Act.

Disclosures Related to the Individual

Paragraph (a) under subsection 29(1) allows custodians to disclose personal health information for the purpose of providing or, assisting in providing, health care to the individual. This type of disclosure is permitted without the consent of the individual. We have concerns about the individual's lack of ability, under the legislation, to control disclosures of personal health information to other health care providers. Under the legislation, health care providers have the discretion to disclose whatever personal health information they deem to be appropriate, under the circumstances.

In the initial drafts of the legislation, individuals were permitted to prevent disclosures of personal health information without their consent for health care purposes. This so-called "lock box," which would provide individuals with some control over disclosures of their personal health information, is a key component of privacy protection. In the absence of any ability to control what information is shared among health care providers, in some cases extremely sensitive, subjective, personally damaging, irrelevant, or outdated personal health information could be shared against the wishes of the individual.

We recognize that the inclusion of the lock box could, in some cases, allow individuals to withhold key personal health information that may be critical to their care and treatment. However, it should be noted that providing individuals with the right to prevent disclosures of all or part of their record of personal health information does not necessarily mean that this information could never be shared for health care purposes. It simply means that the information would not automatically flow freely among those persons who are directly or indirectly involved in the individual's health care, without any involvement on the part of the individual. Instead, the individual would have to be consulted and consent obtained, on a case-by-case basis, before the custodian could disclose the locked part of the record for health care purposes.

Allowing health care providers to determine what personal health information to disclose, in every instance, assumes that health care providers always know what should be disclosed in the best interests of individuals. However, the public may not agree with this assumption. The Equifax Canada Report on Consumers and Privacy in the Information Age (1994) indicated that close to one in five Canadians (18%) reported experiencing improper disclosures of their personal medical information. Respondents to the survey most frequently (8%) stated that a doctor who had treated them or their families had disclosed medical information about them in an improper way.

As individuals increasingly have greater access to a broad range of health information through resources such as the Internet, they can and will play a greater role in their own health and well-being. Accordingly, the legislation should not prevent individuals from being able to exercise some degree of control over what information is disclosed to health care providers.

There is some evidence to suggest that people may withdraw from full participation in their own health care if they are afraid their personal health records will fall into the wrong hands and lead to discrimination, loss of benefits, stigma, and unwanted exposure. A 1999 survey by the California HealthCare Foundation found that one in six people engages in what they refer to as "privacy protective behaviour" to shield themselves from the misuse of their personal health information. This privacy protective behaviour may include lying to doctors, providing inaccurate information, doctor-hopping, and avoiding medical care altogether. If, under the legislation, individuals are able to control what information is disclosed to health care providers, it is more likely that this type of behaviour would be minimized.

As noted above, unlike health information legislation from Alberta and Saskatchewan, Ontario's legislation does not provide individuals with any means of prohibiting the transmission of their personal health information over electronic networks. To some extent, the recommended lock box would compensate for this, by providing individuals with some degree of control over how their personal health information is shared. Health information legislation in Manitoba, which has been in force for sometime, contains a lock box provision whereby individuals can prevent their personal health information from being shared among health care providers without their consent. In the absence of the lock box or any means for individuals to prevent their personal health information from being made available over computerized networks, Ontario's legislation will not provide the same standard of privacy protection provided in other jurisdictions in Canada.

Disclosures about a Deceased Individual

We are pleased the legislation contains provisions that would permit custodians to disclose information about a deceased individual, in certain limited circumstances. These provisions will help to address the concerns raised by the Commissioner, in her 1999 Annual Report, about the inability of family members to obtain timely information about the circumstances of a relative's death. However, we suggest that paragraph (b) under subsection 29(3) may be broader than is necessary

to ensure that those individuals who need to know are informed that an individual is deceased and of the circumstances of the individual's death. In some situations, it may be reasonable to inform a person that the individual is deceased, but not reasonable to inform that person of the circumstances of the individual's death. Accordingly, we recommend that this paragraph be separated into two paragraphs. The first paragraph would permit custodians to inform any person, whom it is reasonable to inform in the circumstances, that the individual is deceased. The second paragraph would permit the custodian to inform any person, whom it is reasonable to inform, of the circumstances of the individual's death, but only if the custodian believes the disclosure does not constitute an unreasonable invasion of the deceased person's privacy or that of any other individual.

To make paragraph 29(3)(d) consistent with this recommendation, the limits on the disclosure of information to family members, to allow them to make decisions about their own health care or their children's health care, should be expanded to ensure that the disclosure does not constitute an unreasonable invasion of the deceased person's privacy or that of any other individual.

Disclosures for Health or Other Programs

Paragraph (a) of subsection 30(1) allows the custodian to disclose personal health information to the Chief Medical Officer of Health or a medical officer of health for the purpose of public health protection or promotion. While we understand the rationale for permitting disclosures of personal health information without the consent of the individual for public health protection, we do not understand why the legislation should also permit disclosures of personally identifiable health information for the purpose of public health promotion. We are not aware of legislation in any other jurisdiction in Canada that permits disclosures of personal health information without the consent of the individual, for the purposes of public health promotion. If disclosures of personal health information for public health promotion are made for the benefit of the individual rather than to protect the public at large, they should be made only with the knowledge and consent of the individual.

Disclosure by the Minister

Subsection 30(5) permits the Minister of Health and Long-Term Care to disclose personal health information for certain purposes relating to the management of the health care system. Subsection 30(6) specifies the safeguards that must be in place before such disclosures are made. In addition to the safeguards noted, we suggest that the Minister should be required to enter into a contractual agreement with the recipient of the information to ensure that the recipient only uses the information for the purpose for which it is being disclosed. If there are some circumstances in which an agreement is not appropriate (e.g., verifying eligibility for health services on a case-by-case basis), then these circumstances should be listed as exceptions to this requirement.

Disclosures Directed by the Minister

We understand the Minister of Health and Long-Term Care may require access to certain information for the purposes of administering and managing the publicly-funded health care system, as provided for under section 31. However, a justifiable concern of the public is that personal information in the custody or control of the government may be used inappropriately for purposes that could adversely affect individuals.

Under the proposed framework, the Minister may require custodians to disclose personal health information or may require a custodian to disclose personal health information to another organization for these purposes. Our review of the legislation indicates that these directed disclosures will be exempted from the general limitations on the collection, use and disclosure of personal health information set out in section 12 (e.g., that the custodian cannot collect, use or disclose more personal health information than is reasonably necessary to meet the purpose). Where the health service is funded, in whole or in part, by the Ministry of Health and Long-Term Care, there is no process for reviewing the directions to disclose issued by the Minister. Also, under the legislation, custodians cannot refuse a direction to disclose issued by the Minister.

We understand that some directed disclosures of personal health information are permitted under current legislation. But, what is being proposed in the legislation, goes well beyond what is currently permitted and is generally too broad. We have seen no convincing evidence from the Ministry of Health and Long-Term Care that it requires the broad powers provided by the legislation in order to collect the information needed for the purposes of administering and managing the health system. In addition, no clear rationale has been provided to exclude directed disclosures from the application of the general limiting principles, set out in section 12, and from any oversight by the Commissioner. All other disclosures permitted by the legislation, without the consent of the individual, will be subject to these important safeguards. Accordingly, unless they can be clearly justified, we recommend eliminating the provisions enabling directed disclosures.

However, if sufficient justification is provided and directed disclosures are permitted, strong privacy safeguards must be incorporated into the legislation. First, there needs to be limits on the amount and type of personal health information a custodian may be directed to disclose. Second, the persons or classes of persons to whom the information may be disclosed should be set out in legislation rather than in regulations. Third, the general limiting principles set out in section 12 must apply to any directed disclosures. Finally, the entire process needs to be open to review by the Commissioner. Specifically, regardless of who funds the health services provided by custodians, the Commissioner should be able to review all directions to disclose personal health information issued by the Minister.

Under the Health Information Act of Alberta, these types of directed disclosures are limited to circumstances where it is authorized by law or where the information relates to government-funded health services. In addition, where the information requested relates to a health service provided by

the custodian, the Department of Health must submit a privacy impact assessment to the Commissioner and consider the comments of the Commissioner before disclosing the information. In addition, the potential recipients are specified in the legislation, rather than regulations. Similar safeguards should be adopted in Ontario if directed disclosures are going to be permitted under the legislation.

In addition, in the limited circumstances that the Commissioner may review a direction to disclose, under subsection 31(2), the 30 days permitted for this review are not sufficient for the Commissioner to elicit representations from the custodian who is being directed to disclose personal health information. The Commissioner should be permitted to extend the time for approving a direction in circumstances when it is necessary to do so.

Subsection 31(7) requires a custodian to comply with a direction to disclose. However, the custodian should be able to refuse a direction and request a review of the direction by the Commissioner where the custodian reasonably believes that the disclosure would constitute an unjustified invasion of privacy. The ability of the custodian to refuse the direction and to request a review by the Commissioner is an important privacy safeguard, regardless of whether the direction has been reviewed by the Commissioner beforehand. This is necessary since the Minister is under no obligation to follow the recommendations the Commissioner made after a review of a direction to disclose.

Disclosures for Research

Section 32 sets out the safeguards for the use and disclosure of personal health information for research. We support the underlying premise that whenever possible, non-identifiable health information should be used for research purposes, and when the use of personal health information is necessary, it should, in general, be with the consent of the individual. We are pleased that, under the legislation, personal health information will be used and disclosed only for research projects that have been approved by a research ethics review body. This approach is consistent with the approach that has been adopted in other jurisdictions in Canada and with the recommendations of the Advisory Council on the Health Infostructure. However, we have a number of suggestions to strengthen the proposed safeguards.

The exceptions to the requirements for research projects are set out in subsection 32(2). This subsection exempts any disclosures made under sections 30 (i.e., disclosures for health and other programs) or 31 (i.e., disclosures directed by Minister). The rationale for these exceptions is not clear. The minimal safeguards, including the requirement of a review by an independent research ethics review body and the establishment of an agreement, should be applied to all disclosures of personal health information for the purposes of research projects or programs, as defined under the legislation. The exclusion of some disclosures, such as the disclosures to Cancer Care Ontario, seriously weakens these safeguards and is unacceptable.

Subsection 32(3) sets out the powers of the research ethics review body and subsection 32(4) describes what the research ethics review body should assess in deciding whether to approve a research project or program. In addition, the research ethics review body should consider whether the proposed research is of sufficient importance to the public interest to clearly outweigh the interest in protecting the privacy of the individuals involved. Such a requirement is contained in Alberta's Health Information Act. Under that legislation, in assessing these competing interests, the review body must consider the extent to which the research contributes to the following:

- identification, prevention or treatment of illness or disease;
- scientific understanding relating to health;
- promotion and protection of the health of individuals and communities;
- improved delivery of health services; or
- improvements in health system management.

Subsection 32(5) states the conditions for requiring consent are to be prescribed in the regulations. However, to ensure adequate public scrutiny, these conditions should be set out in the legislation rather than regulations. In assessing whether the researcher should be required to obtain consent, the research ethics review body should consider the purposes for which the personal health information will be used by the researcher. It may not be necessary to require a researcher to obtain consent, if the personally identifiable health information will be used only for the purpose of linking or matching personal health information across time and/or sources, provided that the following safeguards are put in place:

- the personal health information will only be used for the purpose of linking or matching information;
- the personal health information will be de-identified as soon as the linking or matching procedure has taken place; and
- the personal identifiers will be destroyed or, where the personal identifiers must be retained, safeguards will be put in place to limit access to the personal identifiers once the linking or matching procedure has taken place.

Subsection 32(10) describes what must be contained in a research agreement between the custodian and the researcher. Paragraph (e) states that the researcher agrees not to make contact with individuals unless the individuals have previously consented to being contacted or the custodian authorizes the researcher to contact individuals. The custodian should not be permitted to authorize the researcher to contact the individual. Where the researcher is proposing to contact individuals

directly, the consent of the individual to be contacted by the researcher for that purpose should always be obtained by the custodian beforehand. In addition, the agreement should stipulate that the researcher agrees to permit the custodian to access or inspect the researcher's premises to confirm that the researcher is complying with all of the requirements set out in the agreement. These recommendations are consistent with the approach taken in other jurisdictions, such as Alberta.

Use and Disclosure Outside Ontario

Subsection 37(1) states that a custodian shall not use personal health information outside of Ontario unless certain conditions are met – the use must be permitted in Ontario and the custodian must take appropriate steps to preserve the confidentiality of the information. This section permits the use of personal health information for the purposes permitted under the Act, beyond the boundaries of the province of Ontario. However, this section fails to extend the privacy protection requirements that would apply to that information within the province. To remedy this situation, we recommend the legislation be amended to ensure that any health information custodian who uses personal health information outside of the province will be required to comply with the Ontario legislation.

Subsection 37(2) permits the custodian to disclose personal health information to a person outside Ontario, if certain conditions are met – the disclosure would be permitted if the recipient was in Ontario and the custodian believes the recipient will take appropriate steps to preserve the confidentiality of the information. This subsection permits the use and disclosure of personal health information, for the purposes permitted under the Act, beyond the boundaries of the province of Ontario. However, as with subsection 37(1), this section fails to extend the privacy protection requirements that would apply to that information within the province. To remedy this situation, we recommend that subsection 37(2) be amended by adding paragraph (c) which would require custodians who wish to disclose personal health information outside of the province to enter into an agreement with the recipient of the information stipulating that the recipient must adhere to the requirements of the legislation.

Part VIII: Access to Records of Personal Health Information

Access to Records

This part of the legislation provides individuals with a right to access and request correction of their own personal health information. Under section 44, certain types of records are excluded from the application of this part of the Act. Since the right to access and to request correction of one's own personal health information is an essential component of privacy protection, there should be no mandatory exclusions from this part of the legislation. What are proposed as exclusions should be incorporated into the list of circumstances, set out in section 48(1), under which the custodian has the discretion to refuse to provide access when it is appropriate to do so.

Another concern about section 44 is that, in addition to the types of information specified, paragraphs (d) and (e) allow certain types of personal health information and information in the custody or under the control of a class or classes of custodians to be excluded from this part of the Act by regulation. The legislation should not include broad regulation-making powers of this nature that could fundamentally limit the individual's right of access. Accordingly, paragraphs 44(d) and (e) should be deleted and additional categories of personal health information, if any, to which this part of the Act does not apply should be set out in the legislation.

Section 47 sets out the procedures for accessing one's own personal health information. Subsection 47(3) states that a custodian must respond to a request for access within 30 days. The legislation should also stipulate that a custodian's failure to respond within the required time period will be treated as a decision to refuse access. This would allow the individual to complain to the Commissioner immediately, rather than waiting for the decision of the custodian. Such a provision is contained in comparable legislation from the province of Alberta.

Subsection 47(6) allows the custodian who responds to a request for access not to respond to a subsequent request for the record from the same individual. We do not agree that the custodian should be permitted to not respond to any repeat request for access to a record, regardless of how much time has passed since the initial request. It is possible that individuals may legitimately need to access a record on more than one occasion, for example, if the record has changed.

Under subsection 49(2), if the custodian refuses a request, in whole or in part, the individual is entitled to make a complaint to the Commissioner. In addition, the legislation should include provisions to clarify that the individual can appeal a refusal to correct information that is of a factual nature; a refusal to attach a statement of disagreement to a record where a correction or amendment has been refused; an unreasonable delay in responding to a request for access; an unreasonable or unauthorized fee charged by the custodian; or a refusal to grant a waiver of fees when it is fair and equitable to do so. This would be consistent with public sector privacy legislation and health information legislation from other jurisdictions.

Subsection 48(1) contains a list of circumstances when the custodian may refuse a request for access to one's own personal information. Paragraph (b) allows a custodian to refuse access if the information was collected or created in the course of an inspection, investigation or similar procedure, or primarily in anticipation of or use in a proceeding. In addition, paragraph (c) allows the custodian to refuse access if the access could reasonably be expected to interfere with an inspection, investigation or similar procedure.

Our experience in handling appeals about refusals to grant access to these types of records indicates that the rationale for this exception no longer applies once the inspection, investigation or similar procedure or proceeding has been completed. Accordingly, the custodian should be permitted to refuse access only when access would interfere with an inspection, investigation or similar procedure, as specified in paragraph (c). If paragraph (b) is to be included in the legislation, subparagraphs (i) and (ii) should be further restricted by stating these exceptions apply only if the inspection, investigation or similar procedure or proceeding has not been completed.

Under subsection 48(1) paragraph (f), a custodian is permitted to refuse access if another Act or rule of law prohibits the disclosure. It is not clear what is intended by "another rule of law." Since this subsection already allows custodians to refuse access in a broad range of circumstances, any other "rules of law" that may be applicable under the circumstances should be specified in the legislation.

Amendment of Record

Section 50 sets out procedures for individuals to request amendment of their records of personal health information. Subsection 50(4) permits a custodian to not respond to a repeat request for the same amendment from the same individual. However, the legislation should recognize that, as circumstances change, at some point in time, it may be appropriate for the custodian to reconsider an initial response to a request for an amendment.

Subsection 50(5) requires a custodian who makes a requested amendment to notify anyone to whom the custodian disclosed the information within the preceding year. The custodian does not have to provide this notification if the amendment cannot reasonably be expected to have an effect on the ongoing provision of health care or other benefits to the individual. However, it should be noted that the use and disclosure of personal health information that is not accurate, complete or up-to-date could result in a broad range of adverse consequences to the individual in addition to those specified (e.g., a refusal to provide the individual with health insurance). Accordingly, a broader range of potential harm should be considered before the requirement to give notice of an amendment can be waived. Specifically, the requirement to give notice should be waived only if the custodian reasonably believes that the individual who requested the amendment cannot be harmed in any way if the notification is not provided. Also, there should be a requirement that the individual agree with the notification not being provided. This recommendation is consistent with the Health Information Act of Alberta.

Under subsection 50(8), where a custodian refuses to make a requested amendment, the custodian must attach a statement of disagreement to the record, as prescribed in the regulations. However, in accordance with fair information practices, where a correction or amendment of personal information is refused by a custodian, it is customary for the individual rather than the custodian to decide whether or not a statement of disagreement should be attached to the record and, if so, to determine what should be contained in this statement.

Under Alberta's Health Information Act the custodian must inform the individual of the decision not to correct or amend a record and the individual may either ask for a review of the custodian's decision by the Commissioner or submit a statement of disagreement to be attached to the record. This approach is consistent with the public sector privacy legislation in Ontario.

In addition, when a statement of disagreement is attached to a record, the custodian should be required to provide a copy to any person to whom the custodian has disclosed the record in the year preceding the applicant's request for the correction or amendment. Such a requirement is also consistent with comparable legislation from Alberta, Saskatchewan and Manitoba. As we recommended in cases where a record is amended, the requirement to give notice should be waived only if the custodian reasonably believes that the individual cannot be harmed in any way if the notification is not provided, and the individual agrees.

Under subsection 50(9), the individual is not entitled to complain to the Commissioner, if the custodian either makes the requested amendment or attaches a statement of disagreement to the record. This is not acceptable. If the statement of disagreement is supplied by the custodian, as stated in the legislation, the individual may disagree with its contents and should have recourse to complain. In addition, even if the custodian attaches the statement of disagreement, the individual should be able to ask the Commissioner to review the decision to refuse to make the requested correction or amendment.

Part X: Powers and Duties of the Commissioner

Powers

Section 64 sets out the general powers of the Commissioner. In addition to the stated powers, we recommend that the Commissioner should be able to initiate and conduct privacy audits to ensure compliance with any provision of the Act. This authority is necessary to ensure adequate oversight of the legislation. While subsection 68(6) allows the Commissioner to treat any information as a complaint and to conduct a review, this is not sufficient. In addition, the Commissioner should be able to conduct self-initiated audits using the full investigative powers of the Commissioner, as provided for in the inquiry process under section 69. Privacy audits of this nature are permitted under comparable health information legislation from Alberta, Saskatchewan and Manitoba.

Delegation

Section 65 provides the Commissioner with the necessary authority to delegate any of the Commissioner's powers, duties or functions under the Act. Under subsection 65(1), the Commissioner may delegate powers, duties or functions to the Assistant Commissioner or another employee if there is no Assistant Commissioner. Subsection 65(2) permits the Assistant Commissioner to delegate powers, duties and functions to another employee. One exception under subsection 65(3) is that the Assistant Commissioner may not delegate the duties of the Commissioner under section 31. Section 31 allows the Commissioner to review and comment on any directions to disclose issued by the Minister of Health and Long-Term Care, with respect to non-funded programs or services. The Commissioner is required to respond to the direction within 30 days. However, in some instances, it may not be practically possible for the Commissioner or the Assistant Commissioner to complete this review within the specified time. We recommend that this limitation on the delegation of powers, duties and functions be removed.

Part XI: Administration and Enforcement

Part XI, which sets out the oversight and enforcement regime relating to personal health information, raises a number of grave concerns with us. This Part establishes the powers of the Commissioner to review complaints under the legislation and to conduct inquiries into the decisions of health information custodians relating to access to personal health information. In our view, the provisions of the legislation are seriously inadequate and fail to provide Ontarians with a robust oversight of this most sensitive of personal information.

The investigation that the Commissioner conducted into the disclosure of personal information by the Province of Ontario Savings Office (POSO), tabled with the Legislative Assembly on April 26, 2000, provides ample evidence of the weaknesses of the current public sector oversight mandate. It lacks strong and explicit powers to investigate the complaints of Ontarians and to issue orders when personal information is being used or disclosed in non-compliance with privacy legislation. In the POSO investigation, because of the lack of clear investigative authority and powers, the Commissioner was unable to conduct a thorough investigation into the events that led to the disclosure to private sector firms of sensitive financial information belonging to all account holders. These problems were highlighted by the fact that a number of key individuals refused to be interviewed as part of the investigation. The result was a report that could not satisfy the public's right to know the full details of a public institution's use of personal information that was in non-compliance with the legislation.

The case demonstrates that, without clear authority to conduct an investigation and clear powers to gather the necessary evidence, an oversight body cannot adequately assess the extent to which organizations are complying with their responsibilities. In turn, the public cannot be confident that the custodians of personal information are being held accountable for their information management practices. In the case of the health care sector, which depends on the availability of complete and accurate personal information to function, public confidence in a strong and independent oversight body is critical.

The POSO report highlighted the authority and powers that an effective oversight body requires. Similar authority and powers are essential for the adequate safeguarding of personal health information. This includes explicit power to investigate all complaints, including those relating to the collection, use and disclosure of personal health information, and to issue orders relating to improper uses and disclosures. Without these, the Commissioner will be unable to effectively carry out her mandate, and many of the public's rights and protections under the legislation will be virtually unenforceable.

Complaints

Section 68 sets out the process for complaints under the legislation. Subsection (1) states that any person may complain about any matter under this Act or the regulations or the information practices of a custodian, but not with respect to what constitutes quality of care information. We do not agree that what constitutes quality of care information should not be subject to review by the Commissioner. Under the legislation, the individual does not have a right of access to personal health information that the custodian deems to be quality of care information. However, it is possible that a custodian could apply this exemption in a manner that is not in compliance with the requirements of the legislation. Accordingly, the individual must be able to ask the Commissioner to review the information that the custodian deems to be quality of care information.

Subsection 68(2) states that an individual who makes a complaint to the Commissioner must pay the fee prescribed by the regulations. However, it is our view that individuals should not be charged a fee for making a complaint, as this could present an unreasonable barrier to the Commissioner's processes. The charging of a fee to complain seems particularly inappropriate in cases where the individual is seeking redress for an alleged invasion of privacy.

Under paragraph (b) of subsection 68(3), the Commissioner may require a person who complains to try to effect a settlement with the person about whom the complaint is made within a time period specified by the Commissioner. However, in many cases, it is not possible to determine up-front how complex the issues are and what a reasonable time period would be to try to resolve the issues through mediation. We recommend that the legislation not require the Commissioner to specify a time period. Instead, the Commissioner should have the discretion to specify a time period when it is appropriate to do so.

Subsection 68(13) requires the Commissioner to conduct a review of a complaint in accordance with the procedure prescribed by the regulations. This is not acceptable. Such a provision is unwarranted, could impose serious constraints on the independence of the Commissioner, and would not permit adequate scrutiny by the public. If there is a need to establish review procedures, this should be done in the legislation itself. Otherwise, review processes should be established by the Commissioner. The lack of procedures in the body of the legislation for conducting reviews seems incongruent with the detailed procedures for conducting inquiries, set out in section 69.

The order-making authority of the Commissioner following a review of a complaint is set out in subsection 68(14) under paragraph (b). As noted in the introduction to this Part, the order-making authority is unacceptably narrow and needs to be expanded to ensure compliance with all of the essential requirements of the legislation. Specifically, the Commissioner needs order-making

authority with respect to fees, time extensions, reasonable search, deemed refusals, and all of the use and disclosure practices of custodians. As is the case with public sector privacy legislation, the Commissioner should be able to make orders with any terms and conditions the Commissioner considers appropriate. This also would be consistent with the broad order-making powers provided under health information legislation from other jurisdictions, such as Alberta. Without the recommended order-making powers, the legislation fails to address the concerns raised by the Commissioner in connection with the POSO investigation.

Inquiry

Following a review, the Commissioner may conduct a more formal inquiry into certain types of complaints. The inquiry process is set out in section 69. Subsection 69(1) states that an inquiry may be conducted only if the complaint relates to a request for access or amendment of a record of personal health information. However, it is our strongly held position that the Commissioner must be able to conduct inquiries into complaints about any matter under the Act, rather than just those relating to a request for access or amendment of a record. As the legislation now reads, the Commissioner would be unable to conduct an inquiry, or issue an order, if an individual complained about his or her personal health information being used or disclosed in contravention of the Act. This is unacceptable to us. Our recommended powers would be consistent with the powers of the Commissioner in other jurisdictions, such as Alberta.

Subsection 69(15) states that no person is entitled to have access to or to comment on the testimony or submissions made to the Commissioner by another person, and that the Commissioner shall not authorize or permit any person to contravene this subsection. The second part of this subsection puts unnecessary limits on the Commissioner's capacity to set procedures for resolving complaints. The current appeal process in place under the provincial Freedom of Information and Protection of Privacy Act and the Municipal Freedom of Information and Protection of Privacy Act has successfully incorporated the exchange of submissions between parties. Our experience in resolving appeals and complaints under this legislation indicates that the exchange of testimony and submissions between parties enhances the fairness of the process and facilitates the resolution of issues. This process still allows for information to be withheld where there are valid confidentiality concerns. It is not in the best interests of the public to place this type of limitation on the process for receiving and sharing testimony and submissions among parties during an inquiry into a complaint. This type of restriction on the process is not found in comparable legislation in Alberta and Saskatchewan or in the public sector privacy legislation in Ontario. We recommend deleting that part of subsection 69(15) which states that the Commissioner shall not authorize or permit any person to contravene this subsection.

Consistent with our comments on the order-making authority of the Commissioner in conducting a review (i.e., section 68(14)), the Commissioner's order-making authority following an inquiry, as set out in section 71, is too limited. There should be one section of the legislation dealing with orders that would apply to both reviews and inquiries into complaints. As noted earlier, this section must clearly provide the Commissioner with wide order-making powers. Similar to public sector privacy legislation, the Commissioner should be able to make orders with any terms and conditions the Commissioner considers appropriate. We also recommend that the legislation provides for filing the Commissioner's orders in the Ontario Superior Court of Justice and that these orders be enforceable in the same way as a judgment or order of that court. A similar provision is contained in the Alberta legislation.

Section 72 indicates that the orders and procedures of the Commissioner in conducting reviews and inquiries may be appealed to the Divisional Court. The right of appeal is both unwarranted and unnecessary. Our experience suggests that it is in the best interests of the parties to a complaint, and the public, to be able to rely on the Commissioner's decisions as final, without concern that the process will be unduly extended or made more complicated and expensive by a court process. It is also our view that, in most cases, the right of appeal to the Divisional Court on an issue of law will be used disproportionately by health care custodians, to the detriment of the public. It is our recommendation that, as is the case under public sector privacy legislation, the orders of the Commissioner should be final. There should be no appeal of an order or matter of procedure in a review or inquiry. The Commissioner's decisions would still be subject to judicial review, to permit those cases which raise serious jurisdictional issues to proceed to court. This would be consistent with Alberta's legislation.

Part XII: Miscellaneous

Regulations

The extent to which this legislation creates regulation-making power is an area of great concern to us and one that requires significant amendment. We understand that, in order to implement an effective privacy protection framework, some matters must be reserved for the regulations. However, our review suggests that, at almost every key decision-making point, the legislation includes the ability to deviate from the established rules by way of regulation. For example:

- subsection 14(3)(g) allows for regulations to create exemptions to the computer matching requirements;
- subsection 31(6)(c) allows the Minister to designate, in a regulation, a person to whom the Minister may direct that a disclosure of personal health care information may be made;
- subsections (d) and (e) of section 44 allow certain types of personal health information and personal health information in the custody or under the control of a class or classes of custodians to be excluded from the access provisions of the Act through regulations;
- subsection 68(13) creates the power, by regulation, to prescribe how the Commissioner is required to conduct a review of a complaint; and
- paragraph 26 of subsection 76(1) provides that a regulation may exempt a health information custodian, or a class of them, from any provision of this Act or the regulations.

The regulations could fundamentally alter the operation of the legislation and put serious constraints on the rights of individuals provided by the legislation. Further, these changes could be made without any public scrutiny. Our experience with public sector privacy legislation suggests that the potential for rights and protections granted by a statute, to be later eroded by government action should not be discounted. Accordingly, we recommend significantly narrowing the regulation-making authority provided under the Act. Whenever possible, important issues should be addressed in the body of the legislation.

Additional Recommendations

Privacy Impact Assessment

In Ontario, government organizations are currently required to undertake privacy impact assessments to help determine whether new technologies, information systems, and proposed programs or policies meet basic privacy requirements. In our view, all health information custodians should be required to undertake such assessments. This would be consistent with requirements under health information legislation in other jurisdictions. For example, under Alberta's Health Information Act, each custodian is required to prepare a privacy impact assessment that describes how proposed administrative practices and information systems relating to the collection, use and disclosure of personal health information may affect privacy. This assessment must be submitted to the Information and Privacy Commissioner of that province for review and comment before implementing any new practice or system or changing existing practices or systems. We recommend that similar safeguards should be incorporated in Ontario's legislation.

Conclusion

The health sector depends on the availability of accurate and complete personal health information to provide individuals with the best possible health care. Individuals are generally willing to share this information with their health care providers for this purpose. However, this personal health information can also be useful for a variety of secondary purposes which go beyond the primary purpose of providing care. The use and disclosure of this information for secondary purposes, such as planning and research, is often rationalized by the desire to improved our publicly-funded health care system. Arguably, such uses and disclosures have the potential to benefit us all.

In today's information age, the demand to use and disclose personal health information for secondary purposes is on the rise. But, as this information finds its way outside the health care provider community, concerns over inappropriate and unauthorized collection, use and disclosure mount. When individuals have little or no control over the subsequent uses and disclosures of their personal health information for secondary purposes, their willingness to share this information openly for the primary purpose may be constrained. Accordingly, the challenge is to adequately protect this very sensitive personal information from inappropriate and unauthorized collection, use and disclosure, while, under very limited and controlled circumstances and without unduly infringing on the individual's right to privacy, ensuring that necessary information is available for appropriate secondary purposes that could benefit us all.

While the proposed Personal Health Information Privacy Act provides for the relatively unobstructed flow of personal health information for a range of secondary purposes, it fails to incorporate sufficient safeguards and oversight to ensure that this information is only collected, used or disclosed in a manner that respects the privacy of individuals. To provide an appropriate balance, we believe the legislation should be strengthened in a number of key areas. In general, we recommend the legislation be amended to:

- limit the broad disclosures of personal health information permitted under the legislation, without the consent of the individual;
- limit the number and scope of the regulations that could have a major impact on the overall operation of the legislation; and
- provide sufficient powers for the Commissioner to effectively and efficiently oversee and enforce the legislation.

Our goals in making these recommendations are to ensure that the legislation provides the privacy protections that stakeholders and the public expect; to promote harmonization of this legislation with other provincial legislation and federal privacy legislation; and to facilitate implementation, administration and enforcement of the legislation.

We are committed to working with the Ministry of Health and Long-Term Care and other stakeholder groups in the province to amend this legislation to address all of the issues that have been raised. We believe that with significant amendment this legislation has the potential to provide the protections for personal health information that are becoming increasingly necessary, as the health sector moves into the information age.